IN THE CLAIMS

1. – 36. Canceled.

37. (Currently amended) A method of validating the integrity of a data packet, the method comprising:

decrypting a ~~sub-network layer~~ data packet containing a checksum and a payload ~~to produce a decrypted sub-network layer packet~~;

extracting [[a]] the checksum from the decrypted ~~sub-network layer~~ data packet;

calculating a ~~network layer~~ checksum for ~~a network layer~~ the data packet ~~comprising the sub-network layer packet~~;

comparing the checksum extracted from the decrypted ~~sub-network layer~~ data packet with the ~~network layer~~ calculated checksum; and

detecting a loss of stream cipher synchronization if the ~~network layer~~ calculated checksum does not match the checksum extracted from the decrypted ~~sub-network layer~~ data packet.

38. (Currently amended) The method of claim 37, wherein detecting a loss of stream cipher synchronization if the calculated checksum does not match [[a]] the checksum extracted from the decrypted data packet further comprises:

a network layer of a protocol stack detecting the loss of stream cipher synchronization when the ~~network layer~~ calculated checksum does not match the checksum extracted from the decrypted ~~sub-network layer~~ data packet.

39. (Currently amended) The method of claim 37, further comprising:

comparing the ~~network layer~~ calculated checksum and the checksum extracted from the decrypted ~~sub-network~~ data packet both for a network layer data payload.

40. (Currently amended) The method of claim 37, further comprising:

re-synchronizing a stream cipher with a transmitter of the encrypted ~~sub-network~~ data packet if the ~~network layer~~ calculated checksum does not match the checksum extracted from the decrypted ~~sub-network~~ data packet.

41. Canceled.

42. Canceled.